Health Information Compliance Alert

Enforcement News: CMS Stresses Importance of PECOS Compliance and Cyber Threats

Plus: Think twice about device disposals.

HIPAA requires that practices safeguard their patients' protected health information (PHI), but Medicare wants to remind clinicians that their personal medical and billing information is important, too.

CMS has compiled an MLN Booklet with tips and tools for Medicare clinicians who use the Provider Enrollment, Chain, and Ownership System (PECOS). The guidance, titled "Safeguard Your Identity and Privacy Using PECOS," reminds providers that practice data should be protected to avoid Medicare fraud.

The MLN Booklet touches on several topics that promote privacy. Here's a sampling:

- Revalidation
- Annual PECOS review
- Enrollment checks for false information
- Password protection
- Paper copies for back-up

For more information, you can find the MLN Booklet at www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/ICN-909017-Safeguard-Your-Identity.pdf.

In other news...

Mobile devices are the modus operandi of many thriving practices. They are also vulnerable to cyber attack. That's why when you're ready to upgrade to a new device, you should take particular care on how you dispose of your hardware.

Risk management under HIPAA requires covered entities and their business associates to protect patients' protected health information (PHI), and that includes data available on electronic devices and media, maintains the HHS Office for Civil Rights (OCR) in its July 2018 Cybersecurity Newsletter. "Improper disposal of electronic devices and media puts the information stored on such devices and media at risk for a potential breach," the guidance reminds. "Data breaches can be very costly to organizations."

Assess your disposal rules, analyze and investigate your HIPAA security compliance shortcomings, and then back up your findings with a comprehensive management plan. Because remember, not only do you endanger the livelihood of your practice with shoddy protocols, but you put your patients at risk, too.

Resource: Take a look at the July 2018 issue of the OCR's Cybersecurity Newsletter at www.hhs.gov/sites/default/files/cybersecurity-newsletter-july-2018-Disposal.pdf.